REMARKS/ARGUMENTS

I. Status of Claims

- Claims 1 and 16 are Independent Claims.
- Claims 1 and 16 are currently amended.
- Claims 1-10, 12-24 and 26-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bommareddy et al (US Pat. No. 6,880,089) (hereinafter referred to as **Bommareddy**).
- Claims 11 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over **Bommareddy** in view of Goseva-Popstojanova et al. (US Publ. No. 2003/0033542) (hereinafter referred to as **Goseva-Popstojanova**).

II. Response

Examiner stated in the 11/19/2007 office action that "Applicant has cited different paragraph from the specification to point out how Bommareddy is different from applicant's invention but failed to specifically point out which limitations are not taught by the cited prior art." See Office Action (dated 11/19/2007), p. 3, para. 2, ll. 1-3. This response is aimed to identify those limitations that Bommareddy does not teach.

A. Bommareddy's cleansing cycle involves two major mechanisms, namely operational health monitoring and active detection of firewalls, that are both not taught by the claimed invention self-cleansing mechanism.

The MPEP states that to anticipate a claim, the cited prior art reference must teach every element of the claim. See MPEP § 2131; see also Verdegaal Bros. v. Union Oil Co. of CA, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

As explained in the 8/31/2007 office action response, **Bommareddy** teaches a firewall clustering system that uses internal and external network flow controllers to continually monitor the operational health of firewalls. See **Bommareddy**, Fig. 8, col. 3, ll. 35-37, col. 7, ll. 23-26 and col. 8, ll. 20-22. Apparently, **Bommareddy's** key inventive entity is the network flow controller. It is designed to enforce HTTP traffic redirection to proxy servers, as well as control redirection of other IP traffic. Id. at col. 20, ll. 58-65 and col. 21, ll. 10-15.

To ensure that the servers are operational, these network flow controllers implement server fault-intolerance within a cluster. See **Bommareddy**, col. 21, ll. 17-20. At regular intervals, the network flow controllers would ping each server with application probes and await a reply. Id. at col. 8, ll. 20-26 and col. 21, ll. 16-19. If a server fails to respond, then **Bommareddy** classifies the failed server as being "down." Id. at col. 21, ll. 21-24. If and when a server is down, then the network flow controllers would reroute any packets bound for the down server to the most suitable servers within the cluster. Id. at col. 21, ll. 25-31.

Bommareddy actively looks for firewall failures by using the operational health monitoring feature (i.e., testing the operational state of the firewall with Ping packets). See **Bommareddy**, col. 8, ll. 20-26. For **Bommareddy** to work, **Bommareddy's** firewall clustering system is constantly surveying areas for one or more various failure conditions. These include: "(1) failure of the firewall internal LAN interface and link , (2) failure of the firewall external LAN interface and link, and (3) failure of the firewall due to power outage, software malfunction, hardware malfunction, or other condition." Id. at col. 7, ll. 27-33.

So long as the firewall remains operational, it can be used by internal and external network flow controllers for every inbound and outbound packet. Id. at col. 4, l. 66 – col. 5, l. 2 and col. 9, ll. 13-16. Each of the network flow controllers maintains a list of operational

firewalls. See **Bommareddy**, col. 4, ll. 59-60 and col. 9, ll. 5-7. However, when **Bommareddy's** firewall clustering system discovers or detects a failure, traffic is automatically diverted to the remaining operational firewalls in both inbound and outbound directions. Id. at col. 7, ll. 33-36.

Bommareddy's failure detection/look-out function contrasts that of Applicants' claimed invention. Here, Applicants' key inventive entity, self-cleansing intrusion tolerance system (SCIT), does not actively detect failures in firewalls. Instead, the claimed invention clearly states that subsytems are assumed to have failed. See **Specification**, para. [0022]. There is no need for intrusion detection because SCIT assumes that the server has been compromised as soon as it is connected to an internal and/or external network (e.g., the Internet). See, e.g., **Specification**, paras. [0022], [0047] (assuming that a failure has occurred after being connected to an internal network).

Based on this assumption, Applicants' self-cleansing mechanism enters into an automatic cleansing process by automatically cleansing at least one subsystem (e.g., a firewall, server, gateway, etc.) on a cyclically timed-basis. See **Specification**, Figs. 1-5, paras. [0023]-[0024], [0038]. These self-cleansing activities will occur regardless of whether a fault in an active subsystem is detected or an intrusion into an active subsystem is detected. Id. at para. [0040]. As such, even if an intrusion was successful, the intrusion would be limited to a very short window of one fast, self-cleansing cycle. Id. at paras. [0043], [0044] and [0057].

The main point to take away from this important distinction is that in **Bommareddy**, failure actually exists and that **Bommareddy** is dependent upon and must look for those failures in order for the invention to work.

In sharp contrast, Applicants are neither detecting a failure like **Bommareddy** nor waiting for (or even inducing) a failure. Furthermore, assumption of system failure does not necessarily mean that failure exists. Rather, Applicants' claimed invention just cleanses one or more subsystems regardless of whether failure has occurred. In other words, Applicants' self-cleansing cycles are independent of failure occurrences.

With these major differences in mind, Applicants have amended the independent claims to include in the preamble the limitation of performing routing and cyclical, self-cleansing activities without waiting for or detecting a system failure. Again, without having to wait for or detect a system failure is a key factor of the claimed invention. Because the claimed invention relies on this notion of assumed system failure, these amendments serve as limitations within the preamble that breathes life, meaning and vitality to the amended claims. See Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1305, 51 USPQ2d 1161, 1165-66 (Fed. Cir. 1999) ("If the claim preamble, when read in the context of the entire claim, of, if the claim preamble is 'necessary to give life, meaning, and vitality' to the claim, then the claim preamble should be construed as if in the balance of the claim."); see also MPEP § 2111.02. Support for this limitation can be found in paragraphs [0022], [0043] and [0057] of the Specification.

Bommareddy does not teach this limitation. Nowhere does **Bommareddy** state that cleansing activities can proceed without having to wait for or detect system failures. Instead, **Bommareddy** teaches that firewalls must be examined to determine their operational health status.

Moreover, **Bommareddy** not only lacks these teachings, but **Bommareddy** also teaches an entirely different concept as explained above. These differences lead to one simple

conclusion: **Bommareddy** cannot read upon the claimed invention. Thus respectfully, Applicants request that Examiner withdraw these § 102 rejections.

B. In consideration of Dependent Claims 11 and 25, the combination of Bommareddy and Goseva-Popstojanova teaches away from the claimed invention.

Examiner stated in the 11/19/2007 office action that Applicants were attacking references individually in the 08/31/2007 office action response to show nonobviousness. Applicants had no intention of doing so. Rather, Applicants attempted to point out the differences in **Goseva-Popstojanova** and combine that prior art reference with **Bommareddy** to show how that combination does not teach the claimed invention.

In essence, Applicants hereby reattempt to make the distinction between that combination and the claimed invention. Applicants will first explain what **Goseva-Popstojanova** appears to disclose. Second, Applicants will explain what the combination of **Goseva-Popstojanova** with **Bommareddy** may teach. Third, Applicants will argue how that combination is not the same as Applicants' claimed invention.

Goseva-Popstojanova teaches an intrusion communication network that places emphasis on the continuity of operation and an attack-survivable communication network. See **Goseva-Popstojanova**, Abstract. **Goseva-Popstojanova's** attack-survivable communication network operates in one of the following ways: (1) "entering a vulnerable state from the good state once the communication network becomes vulnerable to intrusion"; (2) "screening for vulnerability to intrusion which would cause the communication network to transition to a vulnerable state to eliminate at least one of the vulnerabilities detected while screening the communication network so as to return the communication network to the good state"; or (3) detecting vulnerabilities by

screening for vulnerability exploitations in the communication network. Id. at paras. [0009]-[0011].

In each of these three ways, **Goseva-Popstojanova's** system enters into a vulnerability state either accidentally or by a user's pre-attacks. See **Goseva-Popstojanova**. para. [0024]. , Needless to say, the strategies for resistance must first fail. Id. at para. [0026]. When either case occurs, **Goseva-Popstojanova** teaches the implementation of four post-attack phases that form the basis of the system's all fault tolerance techniques. Id. at para [0028]. These phases are (a) error detection; (b) damage assessment; (c) error recovery; and (d) fault treatment and continued service. Id. Of relevance to this response are the first two. See Office Action, 6, part 5 (05/31/2007).

Examiner correctly states that **Goseva-Popstojanova** teaches the step of auditing in its system cleansing actions. See **Goseva-Popstojanova**, para. [0029] ("Strategies, for (a) error detection and (b) damage assessment include intrusion detection (i.e., anomaly based and signature based detection), logging, and auditing."). **Goseva-Popstojanova** explains that "auditing provides for an independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changed in controls, policy, or procedures." Id.

If one were to combine **Goseva-Popstojanova** with **Bommareddy**, the combination would likely teach a firewall clustering system that connects two or more firewalls between an internal network and an external network that includes (1) continuous monitoring of the operational health of routers and associated internal and external links, (2) detecting one or more failure conditions, and (3) auditing.

However, as previously argued, **Bommareddy** does not teach the claimed invention because **Bommareddy** depends on looking for failures in the firewall clustering system before entering any cleansing cycle. See supra II.A. With respect to **Goseva-Popstojanova**, which Examiner brings into the combination, **Goseva-Popstojanova's** auditing stage occurs as part of a post-attack phase. In other words, after the system has been attacked, intruded, or detected an attack or intrusion, it would then detect errors and assess damages by detecting other intrusions, logging events and auditing the system. See **Goseva-Popstojanova**, para. [0029]. Therefore, a **Bommareddy** and **Goseva-Popstojanova** combination means that the firewall clustering system must experience some sort of failure and then go through some cleansing cycle before any auditing occurs.

Simply, this combination is not the case seen here. Again, as previously explained, Applicants teach a cleansing system that runs independently. Applicants' claimed invention does not look or wait for any failure to occur first. Contra supra (explaining that both **Bommareddy** and **Goseva-Popstojanova** depend on system failure prior to any cleansing). Instead, Applicants' self-cleaning system just goes ahead and cleans itself. Moreover, auditing can occur at any stage (e.g., during any measurable event, during the self-cleansing stage, during system performance, etc.). See **Specification**, para. [0034].

In identifying **Goseva-Popstojanova's** auditing step, Examiner stated that "it is not necessary the prior art suggest the combination to achieve the same advantage or result discovered by the applicant." See Office Action (dated 11/19/2007), p. 3, para. 3, ll.6-8 (citing MPEP § 2144). Even so, Applicants remind Examiner that the same advantage/result cannot be accomplished here because neither **Goseva-Popstojanova** (viewable as a "failure-dependent type" system with auditing) nor the **Bommareddy-Goseva-Popstojanova** combination

(viewable as a "failure-dependent type" system combined with auditing) teaches the Applicants' claimed invention (viewable as a "failure-independent type" system).

Because of these differences, Applicants believe the combination of **Bommareddy** and **Goseva-Popstojanova** does not read upon Applicants' claimed invention. Therefore, Applicants respectfully request that these § 103 rejections be withdrawn.

C. Dependent Claims 2-15 and 17-27 depend on Independent Claims.

Because Dependent Claims 2-15 and 17-27 ultimately depend on their respective independent claims, the arguments presented for the independent claims also apply to these dependent claims. Therefore, Applicants respectfully request withdrawal of these objections.

Respectfully submitted,

/David Yee, Reg. No. 55,753/
David Yee, Registration No. 55,753

Office of Technology Transfer
George Mason University
4400 University Dr., MSN5G5
Fairfax, VA 22030
Phone/Fax: 703-993-3949

Filed: February 19, 2008